SIATS Journals

Journal of Islamic Studies and Thought for Specialized Researches

(JISTSR)

Journal home page: http://www.siats.co.uk



مجلة الدراسات الإسلامية والفكر للبحوث التخصصية

المجلد 2، العدد 3، اتموز ، يوليو 2016م.

e-ISSN: 2289-9065

Developments of E-government on smart government and the risks and warnings about the applications and programs

Yasser Elmalik Ahmed Seleman

KINGDOM OF SAUDI ARABIA, MINISTRY OF EDUCATION, BISHA UNIVERSITY

Dr.yaserking@hotmail.com

1437هـ – 2016م

ARTICLE INFO

Article history:
Received 9/4/2016
Received in revised form 19/4/2016
Accepted 25/6/2016
Available online 15/7/2016

ABSTRACT

Smart government is a model of evolution of e-government, e-government in general is government public services on the Internet through Web portals applications (Life Events & Business Episodes), smart government and its applications come to complement what has been built and invest in cross closer to citizen on the one hand, the direct and simultaneous interaction with data deployed in society and economic, social and security and its components on the other. Instruments Smart sensors have evolved (Smart Sensors) which are connected to the Internet, such as security surveillance cameras in cities and climate sensors and measuring energy and power associated with the Internet network government consumption.

Smart government is the electronic services digital means for us dispense with many things, including the excessive use of paper and time lost in follow-up transactions between departments is an excellent step in the evolution of government services in the state system and the speed of completion of transactions and customer convenience in first class, which he could accomplish his business through his Smartphone without the need to go to the place of the government department and wait.

1-Introduction

The shift from E-government to smart government needs a lot of continuous work to ensure the readiness of services that will be available to users and requires the administrator to understand the digital needs and how they are applied and completed. Therefore, the study of those needs and understand well the government departments.

Developing or owning a Smartphone application to enter the stage of smart government, if the department does not offer its services properly through electronic pages it is difficult to switch to smart services without going through several stages of development.

Government departments and institutions should first focus on electronic services available on the network, or even non-ready at the moment and develop properly and the use of new technologies and standards, taking into account ease of use and user experience.

The provision of services through several channels including websites, smart phones and text messages and even television.

New developments to lead to a lot of amendments to the e-government model, which is suitable to the harmonic framework updates Data input to the electronic government (Government Interoperability Framework) to match sources and format the new data with back-end systems to the government.



Fig 1: **electronic government needs**

In order to e-government turn into a smart government it will be working on several fronts technical and administrative, including:

• Create a framework for smart government services on mobile phones and how they are assembled and endorsement serve individuals. Smart government services may be provided through a government application of a unified public service it be an element is added or removed so huge or deliberate central government to publish guidance and general guidance on how to develop services and technology to her favourite and how to design and contents of the service and how to protect service (security insurance application and confidential information) and then leave it for devices and various ministries in order to do internally developed smart government services of their own.

• Develop special guidelines smart applications and templates (Smart Government Apps Guidelines). Most governments have developed this special launching governmental Internet sites instructions but so far those governments did not work on the same application-level smart note that the time for citizen interaction with the mobile device far exceeds the time consumed by that citizen interacting with the browsers on desktop devices.

• Work on the huge open government data (Government Big Data) to promote the launch of smart applications around by programmers in the community. An example of this is that the government opens Data trade and economic transactions and the Data and transportation and communication facilities and Data import and export raw form and comes from the programming smart applications on the phones for trader’s service and provide them with information to benefit them in their trade with trading partners in other countries.

• Create data government sensor networks to collect information in real and timely information about security, transport, health, climate, environment and other sectors. With what it means to allocate computing power and Data Centre private to receive process and store the sensor Data.

2-WIRELESS NETWORKING PROBLEMS

In the development researcher discusses a range of topics including:

- Application Programming Interfaces (APIs)

Using application programming interfaces (APIs) to make smart government services or functions are available for use by other applications. Thanks to Smartphone, new services replace traditional

- **Applications and web applications**.

Development of new applications quickly by blending existing services and capabilities in creative ways, is no longer applicable and single user interface, but several interfaces. These interfaces can be built using different techniques, to target different types of users, and can also be built from several interested parties before doing so. In order to enable multiple interfaces, it became the application programming interface (API) base interface for applications, whether old or new. As it has become the new application programming interfaces distribution channel for government services.

-The ability to provide basic functional properties of the work of the APIs, the government entity itself turn into a platform. And here is not enough to provide a set of APIs, it must be those interfaces reliable, scalable and secure at the same time.

-**Security measures relating to the user**

When you provide smart services to the public, should not be overlooked any of the security risks, whether related to the institution or the user, when the development of smart services, taking into account the privacy and security issues related to the participation of sensitive information while using those services. With regard to the user, the service provider must (the government agency, for example) to ensure safe use of the service by the public.

-

3-PROTECTION FOR WIRELESS NETWORK

Security Guidance for encrypting smart applications:

When you develop smart applications, you must take many issues into consideration, including: the use of properties, and the presence of sensitive data, and share information. It should take the necessary security measures in this regard, starting from the development stage, depending on the level of security

necessary for each individual case. Review the instructions below and a number of thorny issues related to security in the development of smart applications.

Protect sensitive data:

• Make sure the rating data stored according to the degree of sensitivity, and then to take security measures accordingly. Perform data processing and storage operations in accordance with those classifications.

• Store sensitive data on the server (server) rather than stored on the client machine, whenever possible, If it is necessary to store data on the client machine, use the application programming interface (API) to encrypt files, which are provided by the operating system, or through other reliable source.

• should always make sure sensitive stored data encryption, as well as the data in the cache (cached).

• In some cases, you can put restrictions on the data as a precautionary measure (to use in a different geographic location, for example).

• For safety reasons, reveal the minimum of user data; namely select the data that will be of benefit to the user, and shapes the rest of the data.



Fig 2: E-government services

Researcher discusses the data protection during transport:

Always assumed that the network layer is safe, and on this basis, has taken the necessary precautions.

• When a specific application to send sensitive data wired or wirelessly, makes use of a secure channel for data transfer between two parties (SSL / TLS) is a prerequisite.

• Use strong encryption algorithms and long keys.

• Ensure that the user interface shows whether the certificates that are used are valid or not.

Usage Analysis and Risk:

• Navigate through the application of the analysis of the basic functions and the method of work. Select network interfaces that the application uses, and select protocols and security standards it uses.

• Select the properties of the machine that could application and opportunities for piracy and potential uses (such as camera, GPS, etc.)

• Check out how he believes in the application of payment information, if it provides this property.

• Identify other applications that interact with smart service, and select applications that may harm the safety and privacy standards.

• Ensure that the source code analysis (source code) for the application, and to identify weaknesses.

• Check out how they carried out the ratification of the user in the application process, and identified potential risks.

• Analyze the data stored within the application process. See the algorithms used in the encryption, and whether vulnerable to known issues.

• Verify that the data that is stored in the cache memory type, and whether sensitive information was stored in the memory.

• tested the application against the "breakthrough talks" attacks in which the attacker between the interlocutors in the network sneaking unbeknownst to either of them (man-in-the-middle) to analyze the possible interventions in the application.

• Check if the sensitive data being leaked to the log files (log files).

• Be sure to maintain the security of the destination server, not the client-side only.

Risks from the perspective of the researcher:

Researcher discusses a range of risks and warnings about the applications and programs

Use smart devices multiple types of applications, the original or private systems and programs. From time to time, these applications and programs make updates or download programs requested in order to add new functionality to it, as is the case in smart phones and tablets. However, these programs and applications may contain vulnerabilities or malicious code. There are many risks associated with the programs and applications can be listed as follows**:**

Applications threats and cipher software and operating systems Installed programs contain smart devices based on certain codes unauthorized procedures.

This code can penetrate the devices by which programs are updated or installed, or applications that are downloaded, or instant messaging, or e-mail.

This code has been inconsistent with the normal operation of the device, or causes the risks of theft or loss of data. Operating systems as well as the risk of a similar, but they may cause greater problems because their influence and ability on the device and the data is much larger than the impact of applications.

Internet threats:

When the devices connected to the Internet, you may reach them malicious code through HTML applications or JavaScript or Flash, or other sources through Web pages that are visited. It may also cause weakness browsers in exposing the devices to the risk of external codes. Take preventive measures such as avoiding users' access to unreliable sites through the use of checks or security certificates at the enterprise level and the use of modern versions of web browsers provides a greater degree of safety. You must modify the settings to suit the security policies in the enterprise. You must make sure not to enter into official websites, but through the means of secure communication. The devices Security Administration is critical of the security structure of the whole enterprise, the risks related devices threaten as well as desktop computers, databases and e-mail devices and servers, networks, and may cause the arrival of unauthorized persons

to sensitive data, or it may cause slow systems. Moreover, because of the mobile nature, the smart devices are prone to loss or theft of data

4-RECOMMENDATIONS

• Data encryption in all communication process to reduce risk wherever possible application of it. However, the encryption method must be compatible with the Federal Information Processing Standard System (FIPS) which does not possess a lot of hardware at the moment. For devices not compliant with FIPS system, institutions must use FIPS 140-2 sandbox security mechanism.
• Provide and encourage the use of formal communication network via virtual private networks (VPN) in high-risk situations, where the authentication and encryption, confidentiality and integrity of secure data across these networks operations.
• must be trained users to be very careful for their effective control on the devices, and that is to give them instructions about the potential for the loss of hardware hazards.
• Ensure that the smart devices do not allow the transaction if we're not connected to the Internet (offline) or to store transaction data for later use. Applications should require it relates to the Internet to complete the transaction.
• For secure smart devices and applications, make sure you download versions concerning the types of new threats and risks
updates.
• Do not have to deal with payment applications other than authorized or can exchange data with applications.

REFERENCES

[1] United Nations Department of Economic and Social Affairs. "United Nations E-Government Survey 2014"(PDF). UN. Retrieved 2014-09-16.
[2] Jump up^ OECD. The e-government imperative: main findings, Policy Brief,

Public Affairs Division, Public Affairs and Communications Directorate, OECD, 2003

[3] Jump up^ Grima-Izquierdo, C. (2010). A generic architecture for e-
E-Democracy: requirements, design and security risk analysis. Government and Ed. LAP Publishing

.)[4] China: The Next, Science Superpower, (2006

[5] Essam Abdel Fattah rain, e-government between theory and practice, the new .2008 University House, Alozartih,

[6] Abdel-Fattah Bayoumi Hijazi, e-government and legal system, the university thought Dar,